

**Notice of Allowability**

Application No.

09/829,763

Applicant(s)

SHIBATA ET AL.

Examiner

Art Unit

Ponnoreay Pich

2135

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 3/29/2007.
2. ☒ The allowed claim(s) is/are 1,3-6,8-9.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☒ All    b) ☐ Some\*    c) ☐ None    of the:
    1. ☒ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
    - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
    - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),  
Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit  
of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413),  
Paper No./Mail Date \_\_\_\_\_
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

### EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Howard Sobelman (Reg #: 39,038) on 5/25/2007. The amendments are to overcome possible 112, second paragraph rejections. As per MPEP 713.04, a separate interview summary form is not provided as the content of the interview has been summarized herein.

The application has been amended as follows:

#### IN THE CLAIMS:

1. (currently amended) A decryption device comprising:
  - an internal-key storage section adapted to store an internal-key;
  - a content-key storage section adapted to store content-keys;
  - a determination section adapted to determine whether or not a value of the content-key storage section in its an initial state and a current value of the content-key storage section are different; and
  - an operation section, the operation section including:
    - a first decrypting section adapted to, when an encrypted content-key is input to the operation section, decrypt the encrypted content-key using the internal-key so as to obtain a content-key and store the content-key in the content-key storage section, and

a second decrypting section adapted to, when an encrypted content is input to the operation section and the determination section determines that the value of the content-key storage section in its the initial state and the current value of the content-key storage section are different, decrypt the encrypted content using the current value of the content-key storage section as the content-key so as to obtain a first output data and output the first output data to outside of the decryption device,

wherein the determination section comprises a register for storing a value of the content-key storage section at the time that said register receives a Power On Reset (POR) signal, and

wherein the POR signal is a signal which pulses only once immediately after power-on or immediately after reset, so that the content key storage section is in an the initial state immediately after a corresponding power-on or reset of the decryption device.

5. (currently amended) A decryption device according to claim 1, wherein:

the second decrypting section is further adapted to prevent decryption of the encrypted content when the determination section determines that the value of the content-key storage section in its the initial state and the current value of the content-key storage section are the same.

Art Unit: 2135

6. (currently amended) A method for decrypting encrypted content in a decryption device including an internal-key storage section and a content-key storage section, the method comprising:

storing an internal-key in the internal-key storage section;

storing content-keys in the content-key storage section;

determining whether or not a value of the content-key storage section in its an initial state and a current value of the content-key storage section are different; and

decrypting an encrypted content-key provided to the decryption device by using the internal-key so as to obtain a content-key and storing the content-key in the content-key storage section; and

when it is determined that the value of the content-key storage section in its the initial state and the current value of the content-key storage section are different, decrypting the encrypted content using the current value of the content-key storage section as the content-key so as to obtain a first output data and outputting the first output data to outside of the decryption device,

wherein, for the determination step, a register stores a value of the content-key storage at the time that said register receives a Power On Reset (POR) signal, and

wherein the POR signal is a signal which pulses only once immediately after power-on or immediately after reset, so that the content key storage section is in an the initial state immediately after a corresponding power-on or reset of the decryption device.

9. (currently amended) A method according to claim 6, further comprising:

preventing decryption of the encrypted content when it is determined that the value of the content-key storage section in its the initial state and the current value of the content-key storage section are the same.

The following is an examiner's statement of reasons for allowance: The prior art does not teach a decryption device or method where decryption of content is only performed when a determination section determines that the current value of the content-key storage section is different than the value of the content-key storage in the initial state, wherein the initial state is the state the content-key storage section is in immediately after a power-on reset or reset of the decryption device.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

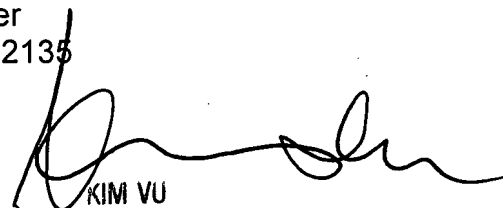
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

PP

Ponnoreay Pich  
Examiner  
Art Unit 2135



KIM VU  
SENIOR PATENT EXAMINER  
TECHNOLOGY CENTER 2100